Office of Information Technology Standard

Security: Authentication / Smart Cards

Definition(s):
Smart cards, which are typically the size of a credit card, provide tamper-resistant storage for protecting a user's certificates and private keys, which provide a very secure means of user authentication, interactive log on, and secure e-mail. A smart card contains a computer chip that could store the user's private key, log on information, and public key certificate used for various purposes, such as digital signatures and data encryption.

Rationale:
Smart card technology offers a reliable alternative to other technologies that have not yet fully developed. Smart cards in conjunction with Public Key Infrastructure (PKI) offer the most secure means of authentication available today.

Approved Standards:

- Smart card solutions must provide a common, interoperable set of extended services and corresponding interfaces that support:
    - Physical and logical access control
    - Biometrics
    - Cryptographic services, including digital signatures and PKI
- Smart card solutions must meet standards allowing interoperability for a variety of devices and multiple applications:
    - Java Card 2.2
    - Open Platform 2.0.1
- Smart card solutions must meet cryptographic standards set by:
    - The National Institute of Standards and Technology
    - The National Security Agency
    - Federal Information Processing Standards Publication 46-3
- Smart card solutions must comply with International Standards Organization (ISO) 7816.

Approved Products:
To be determined. The Office of Information Technology (OIT) intends to establish product standards and master contracts to take advantage of volume pricing for the statewide enterprise.

Guidelines/Technical Considerations:
Smart cards are not mandatory. The Authentication Policy (IT-POL-006) states agencies must use at least one method of authentication. Smart cards may be combined with other authentication methods to create higher levels of security or as a backup. All primary and secondary authentication methods must adhere to IT-POL-006 standards.

Review Cycle:
As needed.

Timeline:
Issued: November 7, 2002

Transition:
Not applicable until product selection.

Procurement:
Until such time that a product standard is selected, agencies must assure that products being considered for purchase comply with the technical specifications listed under Approved Standards. After the product standard is selected, agencies will be required to purchase from the resulting statewide master agreement.

Date: ____________________

Approved by: __________________________________